

Step 1: Investigation Preparation

1. Begin by making a single directory titled Lucky_Duck_Investigations.

```
sysadmin@UbuntuDesktop:~$ mkdir LuckyDuckInvestigations
sysadmin@UbuntuDesktop:~$ cd LuckyDuckInvestigations/
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations$
```

2. In this directory, create a directory for this specific investigation titled Roulette_Loss_Investigation.

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations$ mkdir RouletteLossInvestigation
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations$ ls
RouletteLossInvestigation
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations$
```

3. In Roulette_Loss_Investigation, create the following directories:

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations/RouletteLossInvestigation$ ls
DealerAnalysis PlayerAnalysis PlayerDealerCorrelation
```

- o Player_Analysis to investigate the casino player.

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations/RouletteLossInvestigation$ mkdir PlayerAnalysis
```

- o Dealer_Analysis to investigate the dealers.

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations/RouletteLossInvestigation$ mkdir Dealer Analysis
```

- o Player_Dealer_Correlation to summarize your findings of the collusion.

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations/RouletteLossInvestigation$ mkdir PlayerDealerCorrelation
```

4. Create empty files called Notes_<Directory Name> under each subdirectory to store investigation notes.

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations/RouletteLossInvestigation$ tree
.
├── DealerAnalysis
│   └── Notes_DealerAnalysis
├── PlayerAnalysis
│   └── Notes_PlayerAnalysis
└── PlayerDealerCorrelation
    └── Notes_PlayerDealerCorrelation

3 directories, 3 files
```

Step 2: Gathering Evidence

1. Navigate to the directory where you created the Lucky_Duck_Investigations directory and run the following command to set up the evidence files:
 - o `wget "https://tinyurl.com/3-HW-setup-evidence" && chmod +x ./3-HW-setup-evidence && ./3-HW-setup-evidence`

2. After running this command your current directory should have the following subdirectories:

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations$ wget "https://tinyurl.com/3-HW-setup-evidence" && chmod +x ./3-HW-setup-evidence && ./3-HW-setup-evidence
--2022-04-28 21:24:34-- https://tinyurl.com/3-HW-setup-evidence
Resolving tinyurl.com (tinyurl.com)... 172.67.1.225, 104.20.139.65, 104.20.138.65, ...
Connecting to tinyurl.com (tinyurl.com)|172.67.1.225|:443... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://gist.githubusercontent.com/eddimus/e57fcb9510dd18225142cb23f236da24/raw/39f7f71b22ae7997e92d82e57aedd02bbb6dd481/Setup_Evidence_Files.sh [following]
--2022-04-28 21:24:39-- https://gist.githubusercontent.com/eddimus/e57fcb9510dd18225142cb23f236da24/raw/39f7f71b22ae7997e92d82e57aedd02bbb6dd481/Setup_Evidence_Files.sh
Resolving gist.githubusercontent.com (gist.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.110.133, ...
Connecting to gist.githubusercontent.com (gist.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 32625 (32K) [text/plain]
Saving to: '3-HW-setup-evidence'

3-HW-setup-evidence      100%[=====] 31.86K  --.-KB/s   in 0.006s

2022-04-28 21:24:44 (5.53 MB/s) - '3-HW-setup-evidence' saved [32625/32625]

sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations$ ls
3-HW-setup-evidence  Dealer_Schedules_0310  RouletteLossInvestigation  Roulette_Player_WinLoss_0310
```

3. The Dealer_Schedules_0310 and Roulette_Player_WinLoss_0310 directories contain the dealer schedules and win/loss player data from the roulette tables during the week of March 10.
- Since the losses occurred on March 10, 12, and 15, move the schedules for those days into the directory Dealer_Analysis.
 - Move the files for those days into the directory Player_Analysis.

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations$ tree
.
├── 3-HW-setup-evidence
├── RouletteLossInvestigation
│   ├── DealerAnalysis
│   │   ├── Dealer_Schedules_0310
│   │   │   ├── 0310_Dealer_schedule
│   │   │   ├── 0311_Dealer_schedule
│   │   │   ├── 0312_Dealer_schedule
│   │   │   ├── 0313_Dealer_schedule
│   │   │   ├── 0314_Dealer_schedule
│   │   │   ├── 0315_Dealer_schedule
│   │   │   ├── 0316_Dealer_schedule
│   │   │   └── 0317_Dealer_schedule
│   │   ├── Notes_DealerAnalysis
│   │   └── Roulette_Player_WinLoss_0310
│   │       ├── 0311_win_loss_player_data
│   │       ├── 0313_win_loss_player_data
│   │       ├── 0314_win_loss_player_data
│   │       ├── 0316_win_loss_player_data
│   │       └── 0317_win_loss_player_data
│   ├── PlayerAnalysis
│   │   ├── 0310_win_loss_player_data
│   │   ├── 0312_win_loss_player_data
│   │   ├── 0315_win_loss_player_data
│   │   └── Notes_PlayerAnalysis
│   └── PlayerDealerCorrelation
│       └── Notes_PlayerDealerCorrelation
└── 6 directories, 20 files
```

Step 3: Correlating the Evidence

Complete the player analysis.

1. Navigate to the Player_Analysis directory.

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations/RouletteLossInvestigation$ cd PlayerAnalysis/
```

2. Use grep to isolate all of the losses that occurred on March 10, 12, and 15. Place those results in a file called Roulette_Losses.

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations/RouletteLossInvestigation/PlayerAnalysis$ grep -  
0310_win_loss_player_data 0312_win_loss_player_data 0315_win_loss_player_data > RouletteLosses
```

3. Preview the file Roulette_Losses and analyze the data.

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations/RouletteLossInvestigation/PlayerAnalysis$ cat RouletteLosses  
0310_win_loss_player_data:05:00:00 AM -$82,348 Amirah Schneider,Nola Portillo, Mylie Schmidt,Suhayb Maguire,Millicent Betts,Avi Graves  
0310_win_loss_player_data:08:00:00 AM -$97,383 Chanelle Tapia, Shelley Dodson , Valentino Smith, Mylie Schmidt  
0310_win_loss_player_data:02:00:00 PM -$82,348 Jaden Clarkson, Kaidan Sheridan, Mylie Schmidt  
0310_win_loss_player_data:08:00:00 PM -$65,348 Mylie Schmidt, Trixie Velasquez, Jerome Klein ,Rahma Buckley  
0310_win_loss_player_data:11:00:00 PM -$88,383 Mcfadden Wasin, Norman Cooper, Mylie Schmidt  
0312_win_loss_player_data:05:00:00 AM -$182,300 Montana Kirk, Alysia Goodman, Halima Little, Etienne Brady, Mylie Schmidt  
0312_win_loss_player_data:08:00:00 AM -$97,383 Rimsha Gardiner,Fern Cleveland, Mylie Schmidt,Kobe Higgins  
0312_win_loss_player_data:02:00:00 PM -$82,348 Mae Hail, Mylie Schmidt,Ayden Beil  
0312_win_loss_player_data:08:00:00 PM -$65,792 Tallulah Rawlings,Josie Dawe, Mylie Schmidt,Hakim Stott, Esther Callaghan, Claron Villanueva  
  
0312_win_loss_player_data:11:00:00 PM -$88,229 Vlad Hatfield,Kerys Frazier,Mya Butler, Mylie Schmidt,Lex Oakley,Elin Wornald  
0315_win_loss_player_data:05:00:00 AM -$82,844 Arjan Guzman,Sommer Mann, Mylie Schmidt  
0315_win_loss_player_data:08:00:00 AM -$97,001 Lilianna Devlin,Brendan Lester, Mylie Schmidt,Blade Robertson,Derrick Schroeder  
0315_win_loss_player_data:02:00:00 PM -$182,419 Mylie Schmidt, Corey Huffman
```

- Record in the Notes_Player_Analysis file:
 - The times the losses occurred on each day.
 - If there is a certain player that was playing during each of those times.
 - The total count of times this player was playing.

```
GNU nano 2.9.3 Notes_PlayerAnalysis  
#The times the losses occurred on each day.  
5:00AM, 8:00AM, 2:00PM, 8:00PM, 11:00PM  
  
#Is there a certain play that was playing during each of those times?  
Mylie Schmidt  
  
#The total count of times that this player was playing.  
13
```

Complete the dealer analysis.

1. Navigate to the Dealer_Analysis directory.

```
sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations/RouletteLossInvestigation$ cd DealerAnalysis/
```

2. This file contains the dealer schedules for the various Lucky Duck casino games: Blackjack, Roulette, and Texas Hold 'Em.
 - Preview the schedule to view the format and to understand how the data is separated.

The schedules are broken down into five fields, highlighting the time of a given game, whether it happened at night or daytime (AM/PM), and the first & last name of the blackjack, roulette, and Texas Hold'Em dealers respectively.

```

sysadmin@UbuntuDesktop:~/LuckyDuckInvestigations/RouletteLossInvestigation/DealerAnalysis/Dealer_Schedules_0310$ cat dealer_schedule
Hour AM/PM      Blackjack_Dealer_FNAME LAST      Roulette_Dealer_FNAME LAST      Texas_Hold_EM_dealer_FNAME LAST
12:00:00 AM      Izabela Parrish Marlene Mcpherson      Madina Britton
01:00:00 AM      Billy Jones      Saima Mcdermott Summer-Louise Hammond
02:00:00 AM      Summer-Louise Hammond Abigale Rich      John-James Hayward
03:00:00 AM      John-James Hayward Evalyn Howell      Chyna Mercado
04:00:00 AM      Chyna Mercado      Cleveland Hanna Katey Bean
05:00:00 AM      Katey Bean      Billy Jones      Evalyn Howell
06:00:00 AM      Evalyn Howell      Saima Mcdermott Cleveland Hanna
07:00:00 AM      Cleveland Hanna Abigale Rich      Billy Jones
08:00:00 AM      Rahima Figueroa Billy Jones      Madina Britton
09:00:00 AM      Marlene Mcpherson      Cleveland Hanna Summer-Louise Hammond
10:00:00 AM      Izabela Parrish Madina Britton      John-James Hayward
11:00:00 AM      Madina Britton      Summer-Louise Hammond Chyna Mercado
12:00:00 PM      Summer-Louise Hammond John-James Hayward      Katey Bean
01:00:00 PM      John-James Hayward Chyna Mercado      Evalyn Howell
02:00:00 PM      Chyna Mercado      Billy Jones      Cleveland Hanna
03:00:00 PM      Katey Bean      Evalyn Howell      Rahima Figueroa
04:00:00 PM      Evalyn Howell      Cleveland Hanna Billy Jones
05:00:00 PM      Billy Jones      Rahima Figueroa Summer-Louise Hammond
06:00:00 PM      Rahima Figueroa John-James Hayward      John-James Hayward
07:00:00 PM      Marlene Mcpherson      Chyna Mercado      Chyna Mercado
08:00:00 PM      Saima Mcdermott Billy Jones      Katey Bean
09:00:00 PM      Abigale Rich      Evalyn Howell      Billy Jones
10:00:00 PM      Evalyn Howell      Katey Bean      Cleveland Hanna

```

- Using your findings from the player analysis, create a separate script to look at each day and time that you determined losses occurred. Run all of the scripts and append those results to a file called Dealers_working_during_losses.

```

GNU nano 2.9.3      Dealers working during losses.txt
#March 10th Losses
05:00:00 AM Billy Jones
08:00:00 AM Billy Jones
02:00:00 PM Billy Jones
08:00:00 PM Billy Jones
11:00:00 PM Billy Jones

#March 12th Losses
05:00:00 AM Billy Jones
08:00:00 AM Billy Jones
02:00:00 PM Billy Jones
08:00:00 PM Billy Jones
11:00:00 PM Billy Jones

#March 15th Losses
05:00:00 AM Billy Jones
08:00:00 AM Billy Jones
02:00:00 PM Billy Jones
08:00:00 PM Billy Jones
11:00:00 PM Billy Jones

```

4. Preview your file Dealers_working_during_losses and analyze the data.

- Record in the Notes_Dealer_Analysis file:

```
GNU nano 2.9.3 Notes_DealerAnalysis
#The primary dealer working at the times where losses occurred.
#Billy Jones

#How many times the dealer worked when major losses occurred.
#15 Times
```

5. Complete the player/employee correlation.

- In the notes file of the Player_Dealer_Correlation directory, add a summary of your findings noting the player and dealer you believe are colluding to scam Lucky Duck. Make sure to document your specific reasons for this finding.

```
GNU nano 2.9.3 Notes_PlayerDealerCorrelation
Final Findings:

Mylie Schmidt & Billy Jones are the player/dealer duo conducting the scamming of the casino.
This is due to Mylie appearing in every day there are losses by gamblers, and Billy appearing
in every time slot where losses occurred.

It's also clear because both Mylie & Billy were at the same tables at the same times.
```

Step 4: Scripting Your Tasks

- Remain in the Dealer_Analysis directory. Develop a shell script called roulette_dealer_finder_by_time.sh that can analyze the employee schedule to easily find the roulette dealer at a specific time.

You will be using a script similar to the one you created for the dealer analysis step, but you will not output the results into a file.

- Design the shell script to accept the following two arguments:
 - One for the date (four digits)
 - One for the time
 - Note: The argument should be able to accept a.m. or p.m.

```
GNU nano 2.9.3 roulette_dealer_finder_by_time.sh
#!/bin/bash

#The following script will analyze employee schedules to find roulette dealers specific times.
#Notes: This can accept two arguments (date & time), and cannot accept AM or PM.

grep $2 $1_Dealer_schedule | grep $3 | awk -F" " '{print $5" "$6}'
```

